



CHAPTER 8

Configuring Interfaces in Multiple Mode

This chapter describes how to configure and enable physical Ethernet interfaces, how to create redundant interface pairs, and how to add subinterfaces in the system configuration. If you have both fiber and copper Ethernet ports (for example, on the 4GE SSM for the ASA 5510 and higher series adaptive security appliance), this chapter describes how to configure the interface media type.

For each interface assigned to a context (physical, redundant, or subinterface), this chapter tells how to configure a name, security level, and IP address (routed firewall mode only).



Note

To configure interfaces in single context mode, see [Chapter 7, “Configuring Interfaces in Single Mode.”](#)

This chapter includes the following sections:

- [Configuring Interfaces in the System Configuration \(Multiple Mode\)](#), page 8-1
- [Allocating Interfaces to Contexts](#), page 8-7
- [Configuring Interface Parameters within each Context \(Multiple Mode\)](#), page 8-7

Configuring Interfaces in the System Configuration (Multiple Mode)

In multiple context mode, you configure physical interface parameters and add redundant interfaces and subinterfaces in the system execution space.

This chapter includes the following sections:

- [Configuring Physical Interfaces in the System Configuration \(Multiple Mode\)](#), page 8-2
- [Configuring Redundant Interfaces in the System Configuration \(Multiple Mode\)](#), page 8-3
- [Configuring VLAN Subinterfaces and 802.1Q Trunking in the System Configuration \(Multiple Mode\)](#), page 8-5
- [Enabling Jumbo Frame Support for the ASA 5580 in the System Configuration \(Multiple Mode\)](#), page 8-7

**Note**

If you use failover, you need to assign a dedicated interface as the failover link and an optional interface for Stateful Failover on the [Failover: Setup](#) tab. (You can use the same interface for failover and state traffic, but we recommend separate interfaces). You can use a physical interface, subinterface, or redundant interface for the failover and state links, as long as they are not assigned to a context. To use a subinterface, do not assign the physical interface to a context.

Configuring Physical Interfaces in the System Configuration (Multiple Mode)

This section describes how to configure settings for physical interfaces, and includes the following topics:

- [Physical Interface Overview, page 8-2](#)
- [Configuring and Enabling Physical Interfaces in the System Configuration \(Multiple Mode\), page 8-3](#)

Physical Interface Overview

This section describes physical interfaces, and includes the following topics:

- [Default State of Physical Interfaces, page 8-2](#)
- [Connector Types, page 8-2](#)
- [Auto-MDI/MDIX Feature, page 8-2](#)

Default State of Physical Interfaces

By default, all physical interfaces are shut down. You must enable the physical interface before any traffic can pass through it (either alone or as part of a redundant interface pair), or through a subinterface. For multiple context mode, if you allocate an interface (physical, redundant, or subinterface) to a context, the interfaces are enabled by default in the context. However, before traffic can pass through the context interface, you must first enable the physical interface in the system configuration according to this procedure.

By default, the speed and duplex for copper (RJ-45) interfaces are set to auto-negotiate.

Connector Types

The ASA 5550 adaptive security appliance and the 4GE SSM for the ASA 5510 and higher adaptive security appliance include two connector types: copper RJ-45 and fiber SFP. RJ-45 is the default.

To use the fiber SFP connectors, you must set the media type to SFP. The fiber interface has a fixed speed and does not support duplex, but you can set the interface to negotiate link parameters (the default) or not to negotiate.

Auto-MDI/MDIX Feature

For RJ-45 interfaces on the ASA 5500 series adaptive security appliance, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled.

Configuring and Enabling Physical Interfaces in the System Configuration (Multiple Mode)

To configure and enable a physical interface, perform the following steps:

-
- Step 1** In the Configuration > Device List pane, double-click **System** under the active device IP address.
- Step 2** On the Context Management > Interfaces pane, click a physical interface that you want to configure, and click **Edit**.
- Step 3** To enable the interface, check the **Enable Interface** check box.
- Step 4** To add a description, enter text in the Description field.
- Step 5** (Optional) To set the media type, duplex, and speed, click the **Configure Hardware Properties** button.
- If you have an ASA 5550 adaptive security appliance or a 4GE SSM, you can choose either **RJ-45** or **SFP** from the Media Type drop-down list.
RJ-45 is the default.
 - To set the duplex for RJ-45 interfaces, choose Full, Half, or Auto, depending on the interface type, from the Duplex drop-down list.
 - To set the speed, choose a value from the Speed drop-down list.
The speeds available depend on the interface type. For fiber interfaces, you can set the speed to Negotiate or Nonegotiate. Negotiate (the default) enables link negotiation, which exchanges flow-control parameters and remote fault information. Nonegotiate does not negotiate link parameters. For RJ-45 interfaces on the ASA 5500 series adaptive security appliance, the default auto-negotiation setting also includes the Auto-MDI/MDIX feature. Auto-MDI/MDIX eliminates the need for crossover cabling by performing an internal crossover when a straight cable is detected during the auto-negotiation phase. Either the speed or duplex must be set to auto-negotiate to enable Auto-MDI/MDIX for the interface. If you explicitly set both the speed and duplex to a fixed value, thus disabling auto-negotiation for both settings, then Auto-MDI/MDIX is also disabled.
 - Click **OK** to accept the Hardware Properties changes.
- Step 6** Click **OK** to accept the Interface changes.
-

Configuring Redundant Interfaces in the System Configuration (Multiple Mode)

A logical redundant interface pairs an active and a standby physical interface. When the active interface fails, the standby interface becomes active and starts passing traffic. You can configure a redundant interface to increase the security appliance reliability. This feature is separate from device-level failover, but you can configure redundant interfaces as well as failover if desired. You can configure up to 8 redundant interface pairs.

All subsequent security appliance configuration refers to the logical redundant interface instead of the member physical interfaces.

This section describes how to configure redundant interfaces, and includes the following topics:

- [Redundant Interface Overview, page 8-4](#)
- [Adding a Redundant Interface in the System Configuration \(Multiple Mode\), page 8-5](#)

Redundant Interface Overview

This section includes overview information about redundant interfaces, and includes the following topics:

- [Default State of Redundant Interfaces, page 8-4](#)
- [Redundant Interfaces and Failover Guidelines, page 8-4](#)
- [Redundant Interface MAC Address, page 8-4](#)
- [Physical Interface Guidelines for Use in a Redundant Interface, page 8-4](#)

Default State of Redundant Interfaces

When you add a redundant interface, it is enabled by default. However, the member interfaces must also be enabled to pass traffic.

Redundant Interfaces and Failover Guidelines

Follow these guidelines when adding member interfaces:

- If you want to use a redundant interface for the failover or state link, then you must configure the redundant interface as part of the basic configuration on the secondary unit in addition to the primary unit.
- If you use a redundant interface for the failover or state link, you must put a switch or hub between the two units; you cannot connect them directly. Without the switch or hub, you could have the active port on the primary unit connected directly to the standby port on the secondary unit.
- You can monitor redundant interfaces for failover; be sure to reference the logical redundant interface name.
- When the active interface fails over to the standby interface, this activity does not cause the redundant interface to appear to be failed when being monitored for device-level failover. Only when both physical interfaces fail does the redundant interface appear to be failed.

Redundant Interface MAC Address

The redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. Alternatively, you can assign a MAC address to the redundant interface, which is used regardless of the member interface MAC addresses (see the [“Configuring Interface Parameters in each Context \(Multiple Mode\)”](#) section on page 8-9 or the [“Configuring Security Contexts”](#) section on page 10-16). When the active interface fails over to the standby, the same MAC address is maintained so that traffic is not disrupted.

Physical Interface Guidelines for Use in a Redundant Interface

Follow these guidelines when adding member interfaces:

- Both member interfaces must be of the same physical type. For example, both must be Ethernet.
- When you add a physical interface to the redundant interface, the name, IP address, and security level is removed.

**Caution**

If you are using a physical interface already in your configuration, removing the name will clear any configuration that refers to the interface.

- If you shut down the active interface, then the standby interface becomes active.

Adding a Redundant Interface in the System Configuration (Multiple Mode)

You can configure up to 8 redundant interface pairs. To configure a redundant interface, perform the following steps:

-
- Step 1** If you are not already in the System configuration mode, in the Configuration > Device List pane, double-click **System** under the active device IP address.
- Step 2** On the Context Management > Interfaces pane, click **Add > Redundant Interface**.
- Step 3** In the Redundant ID field, enter an integer between 1 and 8.
- Step 4** From the Primary Interface drop-down list, choose the physical interface you want to be primary. Be sure to pick an interface that does not have a subinterface and that has not already been allocated to a context.
- Step 5** From the Secondary Interface drop-down list, choose the physical interface you want to be secondary.
- Step 6** If the interface is not already enabled, check **Enable Interface**. The interface is enabled by default. To disable it, uncheck the box.
- Step 7** To add a description, enter text in the Description field. The description can be up to 240 characters on a single line, without carriage returns. For multiple context mode, the system description is independent of the context description. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description. The fixed description overwrites any description you enter here if you make this interface a failover or state link.
- Step 8** Click **OK**.
-

Configuring VLAN Subinterfaces and 802.1Q Trunking in the System Configuration (Multiple Mode)

This section describes how to configure a subinterface, and includes the following topics:

- [Subinterface Overview, page 8-5](#)
- [Adding a Subinterface in the System Configuration \(Multiple Mode\), page 8-6](#)

Subinterface Overview

Subinterfaces let you divide a physical or redundant interface into multiple logical interfaces that are tagged with different VLAN IDs. An interface with one or more VLAN subinterfaces is automatically configured as an 802.1Q trunk. Because VLANs allow you to keep traffic separate on a given physical interface, you can increase the number of interfaces available to your network without adding additional physical interfaces or security appliances. This feature is particularly useful in multiple context mode so that you can assign unique interfaces to each context.

This section includes the following topics:

- [Default State of Subinterfaces, page 8-6](#)

- [Maximum Subinterfaces, page 8-6](#)

Default State of Subinterfaces

When you add a subinterface, it is enabled by default. However, the physical or redundant interface must also be enabled to pass traffic (see the “[Configuring Physical Interfaces in the System Configuration \(Multiple Mode\)](#)” section on page 8-2 to enable physical interfaces. See the “[Configuring Redundant Interfaces in the System Configuration \(Multiple Mode\)](#)” section on page 8-3 to enable redundant interfaces).

Maximum Subinterfaces

To determine how many subinterfaces are allowed for your platform, see [Appendix A, “Feature Licenses.”](#)

Adding a Subinterface in the System Configuration (Multiple Mode)

To add a subinterface and assign a VLAN to it, perform the following steps:

-
- Step 1** If you are not already in the System configuration mode, in the Configuration > Device List pane, double-click **System** under the active device IP address.
 - Step 2** On the Context Management > Interfaces pane, click **Add > Interface**.
 - Step 3** From the Hardware Port drop-down list, choose the physical interface to which you want to add the subinterface.
 - Step 4** If the interface is not already enabled, check **Enable Interface**.
The interface is enabled by default. To disable it, uncheck the box.
 - Step 5** In the VLAN ID field, enter the VLAN ID between 1 and 4095.
Some VLAN IDs might be reserved on connected switches, so check the switch documentation for more information. For multiple context mode, you can only set the VLAN in the system configuration.
 - Step 6** In the Subinterface ID field, enter the subinterface ID as an integer between 1 and 4294967293.
The number of subinterfaces allowed depends on your platform. You cannot change the ID after you set it.
 - Step 7** (Optional) In the Description field, enter a description for this interface.
The description can be up to 240 characters on a single line, without carriage returns. For multiple context mode, the system description is independent of the context description. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description. The fixed description overwrites any description you enter here if you make this interface a failover or state link.
 - Step 8** Click **OK**.
-

Enabling Jumbo Frame Support for the ASA 5580 in the System Configuration (Multiple Mode)

A jumbo frame is an Ethernet packet larger than the standard maximum of 1518 bytes (including Layer 2 header and FCS), up to 9216 bytes. You can enable support for jumbo frames for all Gigabit and 10-Gigabit interfaces on interface adapters by increasing the amount of memory to process Ethernet frames. Jumbo frames are not supported on the embedded Management ports. Enabling jumbo frame support might limit the maximum use of other features, such as access lists.

To enable jumbo frame support, go to the Configuration > Interfaces pane, and click the **Enable jumbo frame support** check box.



Note

Changes in this setting require you to reboot the security appliance.



Note

Be sure to set the MTU for each interface that needs to transmit jumbo frames to a higher value than the default 1500; for example, set the value to 9000. See the “[Configuring Interface Parameters in each Context \(Multiple Mode\)](#)” section on page 8-9 to configure the MTU within each context.

Allocating Interfaces to Contexts

To allocate interfaces to contexts, see the “[Configuring Security Contexts](#)” section on page 10-16.

Configuring Interface Parameters within each Context (Multiple Mode)

Within each context, you configure the name, security level, and IP address of each interface. You can also enable same security level communication. This section includes the following topics:

- [Interface Parameters Overview](#), page 8-7
- [Configuring Interface Parameters in each Context \(Multiple Mode\)](#), page 8-9
- [Enabling Same Security Level Communication \(Multiple Mode\)](#), page 8-10

Interface Parameters Overview

This section describes interface parameters and includes the following topics:

- [Default State of Interfaces](#), page 8-8
- [Default Security Level](#), page 8-8

Default State of Interfaces

In multiple context mode, all allocated interfaces are enabled by default, no matter what the state of the interface is in the system execution space. However, for traffic to pass through the interface, the interface also has to be enabled in the system execution space. If you shut down an interface in the system execution space, then that interface is down in all contexts that share it.

In single mode or in the system execution space, interfaces have the following default states:

- Physical interfaces—Disabled.
- Redundant Interfaces—Enabled. However, for traffic to pass through the redundant interface, the member physical interfaces must also be enabled.
- Subinterfaces—Enabled. However, for traffic to pass through the subinterface, the physical interface must also be enabled.

Default Security Level

The default security level is 0. If you name an interface “inside” and you do not set the security level explicitly, then the security appliance sets the security level to 100.



Note

If you change the security level of an interface, and you do not want to wait for existing connections to time out before the new security information is used, you can clear the connections using the **clear local-host** command.

Each interface must have a security level from 0 (lowest) to 100 (highest). For example, you should assign your most secure network, such as the inside host network, to level 100. While the outside network connected to the Internet can be level 0. Other networks, such as DMZs can be in between. You can assign interfaces to the same security level. See the [“Enabling Same Security Level Communication \(Multiple Mode\)”](#) section on page 8-10 for more information.

The level controls the following behavior:

- Network access—By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. You can limit access by applying an access list to the interface.

For same security interfaces, there is an implicit permit for interfaces to access other interfaces on the same security level or lower.
- Inspection engines—Some application inspection engines are dependent on the security level. For same security interfaces, inspection engines apply to traffic in either direction.
 - NetBIOS inspection engine—Applied only for outbound connections.
 - SQL*Net inspection engine—If a control connection for the SQL*Net (formerly OraServ) port exists between a pair of hosts, then only an inbound data connection is permitted through the security appliance.
- Filtering—HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).

For same security interfaces, you can filter traffic in either direction.
- NAT control—When you enable NAT control, you must configure NAT for hosts on a higher security interface (inside) when they access hosts on a lower security interface (outside).

Without NAT control, or for some security interfaces, you can choose to use NAT between any interface, or you can choose not to use NAT. Keep in mind that configuring NAT for an outside interface might require a special keyword.

- **established** command—This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.

For some security interfaces, you can configure **established** commands for both directions.

Configuring Interface Parameters in each Context (Multiple Mode)

To add or edit an interface, perform the following steps.

-
- Step 1** In the Configuration > Device List pane, double-click the context name under the active device *IP address* > Contexts.
- Step 2** On the Device Setup > Interfaces pane, click an interface that you want to configure, and click **Edit**. The Add/Edit Interface dialog box appears with the General tab selected.
- Step 3** In the Interface Name field, enter a name up to 48 characters in length.
- Step 4** In the Security level field, enter a level between 0 (lowest) and 100 (highest). See the “[Default Security Level](#)” section on page 8-8 for more information.
- Step 5** (Optional) To set this interface as a management-only interface, check **Dedicate this interface to management-only**.
Through traffic is not accepted on a management-only interface.
- Step 6** If the interface is not already enabled, check **Enable Interface**.
The interface is enabled by default. To disable it, uncheck the box.
- Step 7** To set the IP address, use one of the following options.
In routed firewall mode, set the IP address for all interfaces. In transparent firewall mode, do not set the IP address for each interface, but rather set it for the whole security appliance or context. The exception is for the Management 0/0 management-only interface, which does not pass through traffic. To set the transparent firewall mode whole security appliance or context management IP address, see the [Management IP Address](#) pane. To set the IP address of the Management 0/0 interface or subinterface, use this procedure.
For use with failover, you must set the IP address and standby address manually; DHCP is not supported. Set the standby IP addresses on the Configuration > Device Management > High Availability > Failover > Interfaces tab.
- To set the IP address manually, click **Use Static IP** and enter the IP address and mask.
 - To obtain an IP address from a DHCP server, click **Obtain Address via DHCP**.
 - a. (Optional) To obtain the default route from the DHCP server, check **Obtain Default Route Using DHCP**.
 - b. (Optional) To renew the lease, click **Renew DHCP Lease**.
- Step 8** (Optional) In the Description field, enter a description for this interface.

The description can be up to 240 characters on a single line, without carriage returns. The system description is independent of the context description. In the case of a failover or state link, the description is fixed as “LAN Failover Interface,” “STATE Failover Interface,” or “LAN/STATE Failover Interface,” for example. You cannot edit this description. The fixed description overwrites any description you enter here if you make this interface a failover or state link.

- Step 9** (Optional) To set the MTU, click the **Advanced** tab and enter the value in the MTU field, between 300 and 65,535 bytes.

The default is 1500 bytes. For the ASA 5580, if you set the value above 1500 bytes, be sure to enable jumbo frame support in the system configuration (see the [“Enabling Jumbo Frame Support for the ASA 5580 in the System Configuration \(Multiple Mode\)”](#) section on page 8-7).

- Step 10** (Optional) To manually assign a MAC address to this interface, on the Advanced tab enter a MAC address in the Active Mac Address field in H.H.H format, where H is a 16-bit hexadecimal digit. For example, the MAC address 00-0C-F1-42-4C-DE would be entered as 000C.F142.4CDE.

If you use failover, enter the standby MAC address in the Standby Mac Address field. If the active unit fails over and the standby unit becomes active, the new active unit starts using the active MAC addresses to minimize network disruption, while the old active unit uses the standby address.

By default, the physical interface uses the burned-in MAC address, and all subinterfaces of a physical interface use the same burned-in MAC address. A redundant interface uses the MAC address of the first physical interface that you add. If you change the order of the member interfaces in the configuration, then the MAC address changes to match the MAC address of the interface that is now listed first. If you assign a MAC address to the redundant interface using this field, then it is used regardless of the member interface MAC addresses.

If you share an interface between contexts, you can assign a unique MAC address to the interface in each context. This feature lets the security appliance easily classify packets into the appropriate context. Using a shared interface without unique MAC addresses is possible, but has some limitations. See the [“How the Security Appliance Classifies Packets”](#) section on page 10-2 for more information. You can assign each MAC address manually, or you can automatically generate MAC addresses for shared interfaces in contexts. See the [“Automatically Assigning MAC Addresses”](#) section on page 10-17 to automatically generate MAC addresses. If you automatically generate MAC addresses, you can use this option to override the generated address.

For interfaces that are not shared, you might want to assign unique MAC addresses to subinterfaces. For example, your service provider might perform access control based on the MAC address.

- Step 11** Click **OK**.

Enabling Same Security Level Communication (Multiple Mode)

By default, interfaces on the same security level cannot communicate with each other. Allowing communication between same-security interfaces lets you configure more than 101 communicating interfaces. If you use different levels for each interface and do not assign any interfaces to the same security level, you can configure only one interface per level (0 to 100).



Note

If you enable NAT control, you do not need to configure NAT between same security level interfaces.

If you enable same security interface communication, you can still configure interfaces at different security levels as usual.

You can also enable communication between hosts connected to the same interface.

- To enable interfaces on the same security level to communicate with each other, from the Configuration > Interfaces pane, check **Enable traffic between two or more interfaces which are configured with same security level**.
- To enable communication between hosts connected to the same interface, check **Enable traffic between two or more hosts connected to the same interface**.

